Transfer Impact Assessment for BlackLine Customers

December 2, 2022

Thank you for your enquiry regarding our use of the Standard Contractual Clauses as a mechanism to receive and process Customers' Personal Data from the European Economic Area ("**EEA**"), United Kingdom ("**UK**") and Switzerland (collectively, "**Europe**").

In July 2020, the Court of Justice of the European Union ("**CJEU**") invalidated the EU-U.S. Privacy Shield framework as a mechanism to lawfully transfer personal data from the EEA to the United States.

Although Schrems II invalidated the Privacy Shield, the CJEU confirmed that the European Commission's Standard Contractual Clauses remain a lawful transfer mechanism under the GDPR, subject to more stringent conditions. In particular, before transferring personal data under the Standard Contractual Clauses, companies must assess whether their personal data will be protected to a standard that is "essentially equivalent" with European data protection rules, or whether the data exporter and importer must implement "additional safeguards" to protect the personal data to the requisite standard. In light of this ruling, the revised Standard Contractual Clauses issued by the European Commission in June 2021 also include the requirement to perform a transfer impact assessment in the event of cross-border transfers, not only to the U.S., but any third country which does not benefit from an adequacy decision. The CJEU decision was before the end of the Brexit transitional period, so also remains binding in the United Kingdom ("**UK**").

In June 2021, the European Data Protection Board ("**EDPB**") published recommendations on supplemental measures (the "**EDPB Recommendations**") to assist businesses undertaking Transfer Impact Assessments ("**TIAs**"). While the EDPB Recommendations are non-legally binding, they represent the collective views of the EU data protection supervisory authorities and their guidance to ensure compliance with the Schrems II decision.

BlackLine Systems, Inc. ("**BlackLine**", the "**data importer**" and "**data processor**") has prepared this document to help its customers (the "**data exporters**" and "**data controllers**") assess the risks of transferring their Personal Data that originates from Europe to BlackLine's Hosted Service when relying on the Standard Contractual Clauses.

This document does not amend or form part of our agreement. Please note this document is intended to help BlackLine customers make an independent risk assessment in consultation with their own privacy counsel. It is for informational purposes only and does not constitute legal advice or substitute legal advice based on your specific situation. We encourage our customers to seek legal counsel advice. Regulators and other market participants may come to conclusions that are different from ours.

This information is provided as of the date of publication of this document and does not take into account regulatory changes or updated guidance issued after the date of publication. We will continue to periodically review and revise this document as the regulatory regime develops.

Summary

BlackLine is headquartered in, and utilizes Sub-processors located in, the United States of America[1]. As determined by the European Court of Justice in Schrems II[2], the laws and practices of the U.S. may not ensure an essentially equivalent level of Personal Data protection to EU law. Taking into account the considerations detailed below and the low likelihood of government access to Personal Data and other relevant factors, we consider that the transfer of European Personal Data to BlackLine does not impinge upon the protection of individuals' rights and therefore does not prevent us from fulfilling our obligations as the data importer under the Standard Contractual Clauses.

This document considers and applies (1) the elements in Clause 14 of the Standard Contractual Clause and (2) the non-legally binding recommendations of the European Data Protection Board[3], which state that organizations should take into account the specific circumstances of the transfer, the laws and practices of the third country of destination, the practical experience of the data importer, and the technical and organizational measures implemented when conducting a transfer impact assessment.

Definitions

"**Agreement**" means the master subscription agreement, written services agreement or any other relevant agreement entered into between BlackLine and Customer related to BlackLine's provision of the Hosted Service.

"**Customer**" means the customer entity licensed to use the Hosted Service under the Agreement.

"**Customer Data**" means any electronic data the Customer submits or uploads to the Hosted Service.

"**Data Subject**" means any individual who can be identified by the information collected about them.

"**DPA**" or "**Data Processing Agreement**" means the Data Processing Agreement or similar agreement between the Customer and BlackLine related to the Processing of Personal Data.

"**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

"**Hosted Service**" means BlackLine's online products accessed at a web site designated by BlackLine to which Customer is being granted access under the Agreement.

---

[1] *BlackLine's principal place of business is at 21300 Victory Blvd., 12th Floor, Woodland Hills, CA 91367.*

[2] *Data in Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems* (C-311/18)

[3] *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, adopted on 18 June 2021

"**MSA**" means BlackLine's Master Subscription Agreement available here.

"**Personal Data**" means any information relating to an identified or identifiable person included in Customer Data, which is Processed by BlackLine or a Sub-processor under the Agreement. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Processing**" (or "**Processed**" or "**Process**") means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Sub-Processors**" shall mean any third-party processor engaged by BlackLine to Process Personal Data in order to provide the Hosted Services.

Any other capitalized terms included in this document and not defined herein have the meanings given to them in the Data Processing Agreement, available here.

The Trans-Atlantic Data Privacy Framework

In March 2022, the European Commission and the United States Government announced that they have "agreed in principle" on a new Trans-Atlantic Data Privacy Framework ("**TADPF**") to enable flows of Personal Data from the EU to the U.S. in compliance with the adequacy standards set out by the CJEU. The Framework establishes a new set of rules and binding safeguards to limit U.S. intelligence authorities' access to European personal data to what is necessary and proportionate to protect national security, and to implement a two-tier redress system to investigate and resolve European Data Subject complaints.

On October 7, 2022, the U.S. Government took a substantial step toward implementing the new Framework, issuing an Executive Order and Regulations that confirm that all U.S. signals intelligence activities must be necessary and proportionate, extending new safeguards to all persons, and laying the legal foundation for establishment of the new redress mechanism. The EU Commission has welcomed these as "significant steps" in meeting the concerns raised by the CJEU in the Schrems II decision. Over the coming months, BlackLine expects that the European Commission will prepare and formally adopt a new adequacy decision that will form the foundation of the new Framework. BlackLine intends to take the necessary steps to adopt the TADPF once it is in place.

What is a TIA?

A TIA is a formal risk assessment that is needed for transfers of GDPR-regulated Personal Data to a third country outside of Europe which does not benefit from a relevant adequacy decision. A TIA assesses the privacy risks that public authorities (in particular, national security authorities) may access the Personal Data, as well as mitigating safeguards relating to those risks. TIAs conducted in compliance with the UK GDPR are substantively similar.

Until the European Commission formally adopts an adequacy decision in relation to the U.S. (e.g., the Trans-Atlantic Data Privacy Framework), companies must continue to conduct TIAs for transfers of GDPR-regulated Personal Data from Europe to the U.S. These TIAs can, however, take account of the new Executive Order signed in October 2022.

The responsibility for conducting TIAs primarily sits with the "data exporter". BlackLine's European customers (those in an EEA Member State, the UK and Switzerland), transfer Customer Data to BlackLine's Hosted Service. Customer Data of Customers who chose to have their Customer Data hosted in Europe, never physically leaves Europe, except with the customer's prior authorization, as necessary to provide the Hosted Service initiated by the customer or as necessary to comply with the law or binding order of a governmental body. BlackLine and its Sub-processors may, under certain circumstances, logically access Customer Data from outside Europe (e.g., support tickets). Such logical access, while limited, is considered a "transfer" under the GDPR. It is then BlackLine Systems, Inc. that is the data exporter transferring GDPR-regulated Personal Data to our Sub-processors located outside Europe where necessary.

BlackLine's TIA

This document considers the elements in Clause 14 of the 2021 SCCs and the six-steps endorsed in the EDPB's Recommendations, and outlines how each of these steps applies to Personal Data processed within BlackLine's Hosted Service. The EDPB's six-steps are:

1) Identify the specific circumstances of your transfer of personal data
2) Identify the transfer mechanism relied on
3) Assess the laws and practices of the recipient country as regards public authority access to personal data
4) Adopt supplementary measures
5) Adopt procedural steps
6) Re-evaluate at appropriate intervals

1. Specific Circumstances of Your Transfer

What is the nature of BlackLine's services?

BlackLine is a SaaS provider that provides cloud-based accounts receivable, intercompany financial management, account reconciliation and financial close accounting software which includes Processing and storing customer financial and accounting data (for example, corporate general ledger account information – balances).

The primary data the Customer inputs into the Hosted Service is financial and accounting data pertinent to its financial close. In providing our tool as a data Processor, BlackLine Processes data our customers submit to our Hosted Service. Under this system of "bring your own data" (where BlackLine does not itself upload client data), we cannot know for certain if client uploaded data contains any Personal Data.

Excluding user information (e.g., login credentials such as a user's name, email address and IP address), BlackLine's Hosted Service is not intended to Process Personal Data, but a BlackLine Customer may choose, at its discretion, to include small amounts of Personal Data in a record of financial activity. A best practices approach would be to not include any unnecessary data and for the BlackLine customer to mask/tokenize any sensitive data (e.g., Personal Data) prior to importing to BlackLine. Nonetheless, we are operating on the assumption that Customer Data will contain Personal Data.

To the extent BlackLine Processes Personal Data for its own purposes as a data Controller, the BlackLine Privacy Policy is publicly available here.

What is the nature of the Personal Data transferred?

A BlackLine Customer may submit Personal Data to BlackLine's Hosted Service, the extent of which is determined and controlled by the Customer in its sole discretion. Such data may include Personal Data relating to the Customer's employees, contractors, clients, business partners or other individuals whose Personal Data is stored in the Hosted Service. The number of Data Subjects whose Personal Data is being Processed (if any) is determined by the Customer. Please see BlackLine's DPA, available here, for more details on the types of Personal Data.

Sensitive personal data (as defined in the GDPR) or would not be Processed by BlackLine, unless uploaded or provided by the Customer. BlackLine Customers are responsible for ensuring that submission of any special categories of Personal Data, where permitted, complies with applicable laws.

Does BlackLine act as a Processor?

It is for the Customer to determine whether it is acting as a Controller or a Processor in uploading Personal Data to BlackLine's Hosted Service. In both scenarios, BlackLine acts as a (Sub-) Processor within the meaning of GDPR Article 28 and Processes such Personal Data only in accordance with the Customer's documented instructions and in accordance with the terms of the MSA and DPA, including to provide the Hosted Service.

Are Data Subjects made aware of the details of the Processing of their Personal Data?

As a data Processor and in light of the type of services it provides, BlackLine does not know the identities of, or directly communicate with, its Data Subjects whose Personal Data may be contained in Customer Data. Any responsibility for making Data Subjects aware of Customers' Processing of their Personal Data using the BlackLine Hosted Service rests with Customers.

Do you have a Data Protection Officer?

BlackLine has appointed a DPO who is in charge of monitoring data protection compliance within the organization and who reports directly to executive management.

What is the duration of the Processing of Personal Data?

BlackLine will generally Process Personal Data for the duration of the MSA, unless otherwise agreed upon with the Customer in writing.

How long is Personal Data retained?

Customers choose how long to retain Customer Data, including Personal Data, on the Hosted Service. Unless otherwise specified in the Agreement, BlackLine does not delete Customer Data, including Personal Data, during a subscription term, unless the Customer instructs BlackLine to do so. After a Customer's contract with BlackLine terminates, BlackLine deletes Customer Data, including Personal Data, in the manner described in the MSA, available here.

What are the information flows for Personal Data for BlackLine's Hosted Service?

The BlackLine Hosted Services is a cloud-based platform, and Customers can allow their users to access the Hosted Service from virtually anywhere with an internet connection. For these reasons, Personal Data may flow to or from BlackLine from global locations, depending on where the Customers' users are located.

What is the format of Personal Data to be transferred?

Encrypted. All Personal Data is encrypted both at-rest and in-transit. Connection to the Hosted Service is via TLS cryptographic protocols ensuring that our Customers' users have a secure encrypted connection. Please see Section 5 (Identify the technical, contractual and organizational measures to protect the data) below for more information on encryption.

What is the transfer frequency of Personal Data?

BlackLine transfers Personal Data on a continuous basis, as the Hosted Service is used.

Does BlackLine require access to Personal Data in the "clear" (i.e., plain, unencrypted readable form)?

Yes, but only in connection with BlackLine's delivery, support and maintenance of its Hosted Service and with the prior consent of the customer.

How is Personal Data transferred to BlackLine via the Hosted Service?

SFTP, HTTPS and Interface (API).

If Personal Data is hosted/stored on behalf of the Customer, in what format is it hosted/stored?

Encrypted database.

Where is Customer Data hosted?

BlackLine will host your Customer Data in the region that you chose at the time you sign up for your subscription (e.g., the US or Europe). For specific locations, see BlackLine's trust site, located here. The vast majority of our Europe-based Customers chose to have their Customer Data hosted in Europe.

Is Personal Data transferred outside of Europe in connection with the Hosted Service? Are there any relevant onward transfer(s) of Personal Data to third party processors?

BlackLine is headquartered in the United States. We may also use Sub-processors – both BlackLine affiliates and third parties – located outside of Europe for certain services to help provide the Hosted Service. For example, BlackLine provides customer support for our Hosted Service, which necessarily means processing data in multiple time zones.

. A full list of our Sub-processors, and their locations, can be found on BlackLine's trust site located here. BlackLine performs a thorough information security and data protection due diligence review on all Sub-processors and signs a GDPR-compliant data processing agreement with each. BlackLine has implemented appropriate safeguards to ensure that Personal Data from Europe remains protected when it is Processed by our Sub-processors.

What is the Purpose of Transfers of European Personal Data to Countries Outside of Europe?

As mentioned above, BlackLine will host your Customer Data in the region that you chose at the time you sign up for your subscription (e.g., the US or Europe). BlackLine will not host Customer Data in a different region without the Customer's prior authorization, except as necessary to comply with applicable law. Customer Data of Customers who chose to have their Customer Data hosted in Europe, never physically leaves Europe without the Customer's prior authorization, except as necessary to comply with applicable law.

As outlined below, BlackLine and its Sub-processors may, under certain circumstances, logically access Customer Data from outside Europe. Such logical access, while limited, is considered a "transfer" under the GDPR and our privacy program is designed to protect Personal Data at all times when providing the Hosted Service.

- *Customer Implementation & Support*

The purpose of such a transfer could, for example, be to allow a BlackLine employee based in the US providing Customer implementation or support to a European Customer. BlackLine provides implementation services and 24/7 Customer support, including from our headquarters in the US, which necessarily means processing data in multiple time zones. In order to provide implementation services or resolve certain Customer support tickets, the BlackLine implementation or support team may require access to the Customer's BlackLine environment, which may include access to Personal Data submitted by Customers to BlackLine's Hosted Service.

As set forth in BlackLine's Master Subscription Agreement, BlackLine will only access your BlackLine environment: (a) to provide and support your use of the Hosted Service and to prevent or address service or technical problems; (b) as you expressly permit in writing or (c) in order to comply with applicable law.

The frequency of any transfers of Personal Data for Customer support depends on the number and type of support queries raised by the Customer and whether the Customer provides access or not.

- *Technical Operations Support*

To respond to technical or service problems, limited authorized BlackLine personnel may on occasion require remote access to the database tables on which Customers' Customer Data is hosted following strict access and monitoring controls. The following operations may involve accessing the raw data without context contained in the database:

- Management of servers, connections and networks
- Providing technical and networking service
- Maintaining operations
- Troubleshooting hardware issues
- Quality assurance testing

- *Sub-processors' Processing of Customer Data Outside of Europe*

BlackLine offers Customers the ability to store their Customer Data in Europe. However, for some of our BlackLine services and features, Customer Data may be Processed outside of Europe. For example, BlackLine utilizes a Sub-processor in the US to provide infrastructure services for the Intacct Connector. If a European customer chooses to have its data stored in Europe and also subscribes to BlackLine's Intacct Connector, Processing of Customer Data in connection with such connector will be done by the applicable Sub-processor in the US.

2. Identify the Transfer Tools You Are Relying On

Where Personal Data originating from Europe is transferred, BlackLine relies on:

(1) adequacy decisions by the European Commission, the UK government and the Swiss Federal Data Protection and Information Commissioner (e.g., Canada, Japan, Switzerland and the United Kingdom), and
(2) the European Commission's Standard Contractual Clauses (Commission Decision 2021/914 of June 2021) (the "**2021 SCCs**"), and the UK International Data Transfer Addendum and Swiss Addendum to the 2021 SCCs, which include the required language to validate the 2021 SCCs for UK and Swiss data protection laws, and
(3) other legally adequate transfer mechanisms recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data.

The 2021 SCCs were specifically drafted by the European Commission and approved by all EU member states subsequent to the Schrems II decision in order to provide appropriate safeguards to allow for a lawful international transfer of Personal Data.

The following countries have not currently been declared adequate by the European Commission, and BlackLine and its Sub-processors will rely on the Controller to Processor or Processor to Processor SCCs to transfer Personal Data to these countries: the United States of America, Australia, Singapore, Mexico and India.

The 2021 SCCs, UK IDTA and Swiss Addendum form part of our DPA with our Customers – please see BlackLine's Data Processing Agreement, available here.

3. Assess Whether the Transfer Tool Relied Upon is Effective in the Circumstances

While performing a TIA, data exporters should assess whether the relevant personal data will be protected to an essentially equivalent or substantially similar standard when processed outside of Europe. Data exporters are required, on a case-by-case basis, to evaluate whether the laws or practices of the recipient country relating to public authority access to data impinge on the effectiveness of the transfer mechanism.

While relying on the 2021 SCCs, BlackLine and its Sub-processors will Process Personal Data in the following non-EEA countries: United States, Australia, Singapore, Mexico and India. This Section 3 summarizes our analysis of the government access policies in these countries and describes any laws that could impede our ability to comply with appropriate safeguards under the 2021 SCCs, any laws that could impinge on the data protection rights of individuals whose data is transferred, and whether these countries have implemented legislation or executive powers that enable government authorities to access Personal Data for criminal law enforcement, security and surveillance purposes.

A. Transfers to the United States of America

The Schrems II ruling has focused European attention on the breadth of law enforcement powers, particularly with respect to national security programs that permit US government agencies to engage in proactive surveillance. This concern is also reflected in the subsequently issued 2021 SCCs. BlackLine understands that the U.S. government's surveillance activities under Section 702 of the Foreign Intelligence Surveillance Act ("**FISA 702**") and U.S. Executive Order 12333 ("**EO 12333**") were held by the CJEU in July 2020 to fall short of the level of protection required by the GDPR. As such, these statutes may be regarded as problematic.

BlackLine's headquarters is located in the U.S. and, thus, is subject to personal jurisdiction within the U.S. It could potentially be compelled under U.S. criminal law to produce to U.S. law enforcement materials that are accessible to it or that are otherwise within its possession, custody, or control. BlackLine also could potentially be compelled to produce to U.S. intelligence authorities certain data in response to FISA 702 and certain other electronic surveillance provisions of FISA.

However, further information on the operation of these laws has been declassified by the U.S. government since the Schrems II ruling. For example, it is noted that FISA 702 applies to certain kinds of entities (more on this below), and EO 12333—where it is relevant for direct access cases—can be addressed through appropriate encryption in transit, so many types of transfers remain unaffected.

In addition, these surveillance activities are subject to the restrictions imposed by U.S. Executive Order 14086 ("**EO 14086**") signed in October 2022 after the Schrems II ruling. EO 14086 restricts all such activities to those which are necessary and proportionate and implements new safeguards including a binding and independent redress mechanism. For more details, please see The White House Fact Sheet.

Executive Order 12333 ("EO 12333")

EO 12333 authorizes U.S. intelligence agencies to conduct surveillance outside the U.S. by collecting foreign intelligence information from communications infrastructure, including data transmitted by radio, wire, and other electromagnetic means. Essentially, EO 12333 relies on U.S. intelligence agencies' technical ability to gain direct access to telecommunications infrastructure.

It is important to note that bulk data collection, the type of data collection at issue in Schrems II, is expressly prohibited under EO 12333. EO 12333 doesn't authorize the U.S. government to compel private companies (such as BlackLine) to assist the government or to disclose Personal Data. Therefore, neither BlackLine nor its Sub-processors would have any legal obligation to assist the U.S. government in conducting surveillance if the government relied on EO 12333 to request Personal Data. BlackLine contractually commits to its customers that it will not do so voluntarily (see Step 4 below). As a result, BlackLine does not and cannot be ordered to take any action to facilitate the type of bulk surveillance under EO 12333 that was considered problematic in the Schrems II ruling.

As the CJEU noted, the primary concern regarding EO 12333 is the US government's ability to collect Personal Data while it is in transit to the US by intercepting data travelling over transatlantic cables. Personal Data can effectively be protected from this type of interception through security measures, such as encryption. BlackLine addresses this risk today by encrypting Personal Data. BlackLine ensures that all Personal Data is encrypted using secure encrypted transmission protocols and algorithms both at-rest and in-transit (for more detail see Step 4 below). Additionally, BlackLine has not built any backdoors to allow government authorities to circumvent its security measures to gain access to Personal Data.

Further, the surveillance activities under EO 12333 are subject to the additional safeguards and protections required by the October 2022 Executive Order.

FISA Section 702

The U.S. government uses provisions under FISA 702 to gain access to certain data related to national defense and security. In particular, FISA 702 can be used to obtain "foreign intelligence" information about foreign adversaries, including the plans and identities of

terrorists and terrorist organizations, the intentions and capabilities of weapons proliferators and spies, and cybersecurity efforts by foreign actors against the U.S. Particularly since the October 2022 Executive Order, U.S. law requires that any exercise of this authority is necessary and proportionate and subject to appropriate safeguards.

BlackLine believes Personal Data is unlikely to constitute “foreign intelligence” information under FISA 702 because it’s not the type of information the U.S. government appears to be primarily seeking in order to protect against attacks by foreign powers.

We would like to point our Customers to the white paper from the US Department of Commerce, Department of Justice, and Office of the Director of National Intelligence. The white paper outlines the limits and safeguards in the US relating to government access to data in response to the Schrems II ruling, notably that companies like BlackLine in the business of “ordinary commercial products or services” and whose data transfers “involve ordinary commercial information such as employee, customer, or sales records” have “no basis to believe U.S. intelligence agencies would seek to collect that data” through FISA 702.

These statements are supported by publicly reported cases involving U.S. national security requests, including FISA 702 requests. These demonstrate that the government generally targets data held by consumer-facing electronic communication services providers (e.g., information associated with email, telephone, internet, and social media services), and not commercial information processed by providers of ordinary commercial products and services such as business and workplace software.

For BlackLine, like most companies, the concerns about national security access to Customer Personal Data highlighted by Schrems II are “unlikely to arise because the data they handle is of no interest to the U.S. intelligence community.” Companies handling “ordinary commercial information like employee, customer, or sales records, would have no basis to believe US intelligence agencies would seek to collect that data.” BlackLine provides Customers with accounts receivable, account reconciliation and financial close accounting software. BlackLine believes that it is unlikely that the limited amount of Personal Data contained in Customer Data would be of interest to government intelligence agencies.

FISA Section 702 authorizes “upstream” and “downstream” collection.

Upstream collection authorizes US authorities to collect communications as they travel over the internet backbone. To date, the US Government has interpreted and applied FISA 702 upstream orders to only target market providers that have traffic flowing through their internet backbone and that carry traffic for third parties (i.e., telecommunications carriers).

BlackLine does not provide such backbone services but only carries traffic involving our own Customers. As a result, BlackLine is not eligible to receive the type of orders principally addressed in, and deemed problematic by, the Schrems II ruling.

Downstream collection authorizes US authorities to collect targeted data directly from an Electronic Communications Service Provider ("**ECS**") based in the US. Like any U.S.-based cloud service provider, BlackLine will likely qualify as a Remote Computing Service ("**RCS**") for certain services it provides to customers and will therefore be considered an ECS under FISA 702. But this status doesn't mean that BlackLine has received or is likely to receive a request under FISA. FISA 702 requires an independent court to authorize a specific type of foreign intelligence data acquisition which is generally unrelated to commercial information.

Based on the above, we assess the likelihood of BlackLine receiving any request under FISA 702 as being remote. In the event that US intelligence agencies were interested in the type of data that BlackLine processes, safeguards such as the requirement for authorization by an independent court and the necessity and proportionality requirements would protect Personal Data from excessive surveillance. To the extent BlackLine may be compelled to respond to such a law enforcement request for Personal Data, we will carefully review the request to verify it is lawful and challenge the request, if we conclude it is invalid or unlawful, in accordance with BlackLine's principles and contractual commitments on government access requests as further described below in Step 4.

NSLs & ECPA

National Security Letters ("**NSLs**") can be issued to an ESC without prior judicial oversight under ECPA. However, the U.S. government must certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.

In practice, the nature of the information sought with NSL letters is limited to non-content data: name, address, length of service, and local and long-distance toll billing records. Moreover, an organization receiving an NSL may seek court input and judicial review, upon receipt of such request.

The Electronic Communications Privacy Act ("**ECPA**"), regulates when ECS and RCS may or must disclose user or subscriber records and communications to law enforcement agencies.

Generally, ECPA restricts when an ECS and RCS—such as BlackLine—can freely disclose such information. Communications content (such as email, private messages, photographs, etc.) is generally subject to the strictest rules, and "basic" subscriber information (such as

names of account holders, types of service they receive, etc.) are provided the least protection.

An ECS or RCS can be subject to various types of legal process including a subpoena, court order, court-issued ECPA warrant, pen register, and trap-and-trace court order or a court-issued Title III Wiretap. However, any of these forms of legal process must be either issued by a court or otherwise subject to judicial oversight. An ECS or RCS may be compelled to produce data to U.S. law enforcement for criminal investigative purposes if such data is within its possession, custody, or control regardless of whether such data is stored within or outside of the U.S., and often regardless of whether the ECS or RCS itself is in physical possession of the data.

Generally speaking, U.S. laws (like the Electronic Communications Privacy Act) involve judicial oversight, safeguards and redress mechanisms that are consistent with the level of protection under EU law.

CLOUD Act

The Clarifying Lawful Overseas Use of Data Act ("**CLOUD Act**"), enacted in 2018, clarifies existing legal frameworks and retains meaningful limitations on US law enforcement's ability to request data, for example: Companies must be subject to the jurisdiction of US law enforcement agencies.

The CLOUD Act only permits US government access to data in criminal investigations after obtaining a warrant approved by an independent court based on probable cause of a specific criminal act.

The CLOUD Act does not allow US government access in national security investigations, and it does not permit bulk surveillance. The CLOUD Act further confirms that the physical location of data is not the deciding factor but whether the recipient of a request has "possession, custody, or control" of the data. Requests are subject to the existing high standards and procedures for making such a request.

Lastly, the CLOUD Act also established additional safeguards, including explicitly allowing companies to challenge disclosure requests that conflict with another country's laws.

Generally speaking, the Cloud Act involves judicial oversight, safeguards and redress mechanisms that are consistent with the level of protection under EU law.

Independent and Impartial Oversight System

The CJEU held in the Schrems II judgement that the U.S. government's surveillance activities under FISA 702 and EO 12333 were not subject to an independent and impartial oversight system.

FISA 702 is subject to ongoing oversight by the Foreign Intelligence Surveillance Court and the congressional intelligence committees.

A provider may also seek redress on behalf of its customers by challenging the applicability of FISA 702 or a U.S. governmental request for the party's participation in the FISA 702 program under 50 U.S.C. § 1881a(j).

Right of Redress for Data Accessed by Government Authorities

Once EO 14086 is fully implemented, individuals from qualifying states will have the right to lodge complaints through their relevant public authorities for investigation and resolution by a two-tier redress mechanism that will be able to issue binding resolutions to ensure that any processing of that individual's data is lawful. This strengthens individual enforcement rights and is designed to address the CJEU's concerns in Schrems II that recourse was previously insufficient.

In addition, individuals generally have a right of redress any time information is sought to be used against them in any proceeding, including a criminal proceeding. For example, in the national security context, any person against whom the government intends to use in any type of legal proceeding evidence obtained or derived from electronic surveillance can move to suppress such evidence pursuant to 50 U.S.C. § 1806(e). Additionally, under 50 U.S.C. § 1810, an aggrieved person (other than a "foreign power" or an "agent of a foreign power") who has been subject to surveillance or whose information has been obtained through electronic surveillance and disclosed or used in violation of 50 U.S.C. § 1809 also will have a private right of action for civil damages against any person who committed the violation.

Practical experience dealing with government access requests

The EDPB Recommendations and the 2021 SCCs enable data exporters to take into account the data importer's practical experience "with relevant prior instances of requests for access received from public authorities" when performing their transfer impact assessment.

BlackLine has never received any legal process from U.S. government authorities under FISA, EO 12333 or any other laws authorizing the compelled production of Personal Data.

While BlackLine may technically be subject to the surveillance laws identified in Schrems II, we do not receive these types of requests in our day-to-day business operations.

Based on the above, we assess the likelihood of BlackLine receiving any request under FISA 702 as being remote. To the extent BlackLine may be compelled to respond to such a law enforcement request for Personal Data, we will carefully review the request to verify it is lawful and challenge the request, if we conclude it is invalid or unlawful, in accordance with BlackLine's principles and contractual commitments on government access requests as further described below in Step 4.

Conclusion

Based on the above, BlackLine has no reason to believe that the U.S. laws and practices applicable to the Processing of Personal Data by BlackLine or its Sub-processors prevent BlackLine from fulfilling its obligations under the 2021 SCCs, the UK IDTA, Swiss Addendum to the 2021 SCCs or otherwise pose any materially different privacy risks as to inappropriate disclosure of personal data to foreign government law enforcement and intelligence agencies, including in the U.S.

Furthermore, our assessment has led us to conclude that the risk of such a request breaching a Data Subject's rights is very low. This is particularly in light of the recent October 2022 Executive Order 14086, which has been designed to assuage the concerns remaining in the U.S.'s previous regime for public authority access to data. While the new U.S. regime is yet to be assessed as adequate, the EU Commission has made it clear that this development includes material improvements which improve the safety of transatlantic data flows, and has also made it clear that this will be of immediate benefit in preparing TIAs.

In summary, we believe a combination of objective factors such as the business sectors in which BlackLine's Hosted Service is used, the purposes for which BlackLine transfers and Processes Personal Data, the limited amount of Personal Data Processed within BlackLine's Hosted Service and the general lack of relevance of that data to government intelligence agencies, the measures in Step 4, relevant public statements issued by the U.S. government, publicly reported cases evidencing the past application of U.S. security laws, the documented experiences of other cloud service providers processing comparable personal data, evidence of practices by U.S. authorities, that surveillance laws and regulations that are potentially applicable to BlackLine's Processing of customer Personal Data are unlikely to be applied in practice, BlackLine's own experiences to date, and the improved protections introduced in the October 2022 Executive Order, all strongly support BlackLine's assessment that it can continue to provide adequate protection to data transferred from Europe to the U.S.

Even if BlackLine is compelled to respond to a law enforcement request for Personal Data, we will carefully review the request to verify its legality and challenge the request, if we conclude it is invalid or unlawful, in accordance with BlackLine's principles and contractual commitments on government access requests as outlined in Step 4 below.

This extensive review has been undertaken in line with the EDPB recommendations, which specifically lists these as reliable sources on the application of the law in practice. Therefore, no additional supplementary measures are necessary at this time.

B. *Transfers to Australia*

The use of listening and surveillance devices are regulated by legislation in the Commonwealth, State and Territory levels. These legislations are as follows:

- Commonwealth – *Surveillance Devices Act 2004*; *Telecommunications (Interception and Access) Act 1979*;
- Australian Capital Territory – *Listening Devices Act 1992*;
- Queensland – *Invasion of Privacy Act 1971*;
- New South Wales – *Surveillance Devices Act 2007*;
- Northern Territory – *Surveillance Devices Act 2000*;
- South Australia – *Surveillance Devices Act 2016*;
- Tasmania – *Listening Devices Act 1991*;
- Victoria – *Surveillance Devices Act 1999*; and
- Western Australia – *Surveillance Devices Act 1998*.

Generally, these types of legislation generally prohibit covert telecommunication interceptions and places prohibitions on the use of listening devices and the use of records derived from, as well as the publication, communication and admission into evidence of material relating to, them. We do not consider these legislations to be applicable in respect of BlackLine's Processing of Personal Data under the MSA.

In relation to the *Telecommunications (Interception and Access) Act 1979* (Cth), there are requirements on telecommunications service providers to retain or disclose certain types of metadata for law enforcement and national security purposes. This legislation generally applies to licensed carriers, carriage service providers, and internet service providers. As above, we do not consider this legislation to apply in respect of BlackLine's Processing of Personal Data under the MSA.

Australia has conditions on the access to and use of personal information by public authorities, such as requiring warrants issued by certain judges, the Attorney General or the Director General of Security. The Privacy Commissioner is responsible for oversight and enforcement of the Privacy Act and the 13 Australian Privacy Principles ("**APPs**"), which includes complaints made by individuals about invasions of their privacy and/or breaches of

the APPs. Australia has signed and adopted the following privacy related commitments: International Covenant on Civil and Political Rights; OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; Asia-Pacific Economic Cooperation Privacy Framework; and APEC Cross Border Privacy Rules.

C. ***Transfers to Singapore***

There is a broad framework of common law and statutory torts which provide indirect privacy related interests, such as nuisance, trespass to the person, defamation, law of confidence and the Protection from Harassment Act. Additionally, the Personal Data Protection Act 2012 (No. 26 of 2012) provides a standard of protection for personal data across organizations.

The data protection regulatory framework in Singapore, including enforcement by the Personal Data Protection Commission ("**PDPC**"), provides individuals with a high level of protection and safeguard with respect to their personal data and the processing of personal data by organizations. The Singapore Personal Data Protection Act 2012 ("**PDPA**") provides a broad set of rights and protections for the personal data of Singapore residents. The PDPC has actively investigated and brought enforcement actions for violations of the PDPA. While there are some differences in the scope of protection, BlackLine believes that, on the whole, Singapore's personal data protection legal and enforcement framework provides individuals with an equivalent level of protection as that accorded to individuals by GDPR.

There are statutory laws in Singapore, such as the Criminal Procedure Code, Telecommunications Act, Prevention of Corruption Act, which empower the authorities to access and seize data stored in Singapore, which may include personal data, whether for domestic purposes, or at the request of a foreign country. Depending on the laws in question, there are certain requirements and safeguards put in place in relation to the exercise of such power (example: the requirement of a court order, judicial review by the courts of administrative action, avenues of appeal to the Minister, etc.).

BlackLine has also assessed government access to private data under Singapore law. The Singapore Police have the power to issue written orders requiring a person to produce a document or thing in that person's possession or power if the Police considers that the document or thing to be necessary or desirable for any criminal investigation or proceeding under Singapore law. They can also invoke broader powers to access and use a computer in connection with an investigation of a serious criminal offences. Singapore law does not provide, however, for general powers of mass surveillance to law enforcement authorities; the Singapore Police have only targeted powers of data access or surveillance where the data being sought is necessary for the purposes of the investigation being undertaken by the authorities into a criminal offense. To date, BlackLine has not been the subject of written order, subpoena or other request of the Singapore Police regarding Personal Data stored in Singapore or of Singapore residents.

The Personal Data Protection Commission has been established and appointed to oversee the protection of personal data in Singapore and to administer and enforce the Personal Data Protection Act 2012 (No. 26 of 2012). Singapore has entered personal into the Asia Pacific Economic Cooperation Privacy Framework, which provides principles and implementation guidance on the collection, holding, processing, use, transfer, or disclosure of information. Singapore is also a participant of the APEC Cross-Border Privacy Rules.

Singapore also has procedures to object to or resist requests for personal data. For example, a state authority's request for personal data could potentially be contested via judicial review on the grounds of illegality, irrationality, or procedural impropriety.

D. *Transfers to Mexico*

All public activity is subject to the law and privacy is a fundamental right as per Article 16 of the Constitution of Mexico ("**the Constitution**"). All authorities within the scope of their powers, have the obligation to promote, respect, protect and guarantee human rights in accordance with the principles of universality, interdependence, indivisibility, and progressivity (Article 1 of the Constitution).

In Mexico, all individuals shall be entitled to the human rights granted by the Constitution and the international treaties signed by the Mexican State, as well as to the guarantees for the protection of these rights. This also includes the rights in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), Interamerican Treaties and the International treaties of the Universal Declaration of Human Rights, International Covenant on Civil and Political Rights and American Convention on Human Rights.

The National Center of Intelligence has statutory authority to request information from private parties for intelligence purposes and to conduct surveillance to avert threats to national security. Such surveillance requires advance judicial authorization under prescribed procedures that limit the length and scope of the surveillance.

At local level, there are laws specialized in human rights, some examples being the Federal Law to Prevent and Eliminate Discrimination and the right to due process in Federal Criminal Law. Federal Law on the Protection of Personal Data Held by Private Parties 2010 ("**the Data Protection Law**") and Regulations to the Federal Law on the Protection of Personal Data Held by Private Parties 2011 ("the **Regulations**") protect the privacy rights of individuals and govern data transfers in Mexico.

Among other privacy protections, the Data Protection Law and the Regulations recognize the right to be informed of processing activities and the right to access personal data, and provide that transfers of personal data be governed by a privacy protective agreement and that Data Subjects must be informed of and consent to certain transfers of personal data. The National

Institute for Transparency, Access to Information and Protection of Personal Data ("**INAI**") acts on Data Subject complaints. Furthermore, it is possible for Data Subjects to seek damages in civil courts.

E. *Transfers to India*

India has a few laws that potentially could permit electronic surveillance of Personal Data, for example:

- Implementing Section 5(2) of the Telegraph Act (1885) allows the Indian government to intercept and disclose electronic or telephonic messages on the occurrence of any public emergency or in the interest of public safety.

- Section 69 of the Information Technology Act (2000) allows the Indian government to intercept, monitor, or decrypt any information received or stored through any computer resource if such activity is "necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence."

- Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 ("**Interception Rules**"). The Interception Rules, framed under the Information Technology Act 2000 ("**IT Act**"), prescribes that the Central Government or any State Government in India may authorize a government agency to intercept, monitor and decrypt any information generated, transmitted, received or stored in any computer resource upon being satisfied that it is in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to the above or for investigation of any offence.

- Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules 2009 ("**Monitoring Rules**"). Under the Monitoring Rules, framed under the IT Act, the Central Government in India has authorized certain governmental agencies such as the Indian Computer Emergency Response Team (CERT-In), to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource for the purpose of enhancing cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in India.

The Supreme Court of India has recognized the right to privacy as a fundamental right under the Indian Constitution, which limits the scope of application of these Indian surveillance laws. In particular, under applicable rules, any interception, monitoring or decryption of electronic information by the Indian government must be approved by a competent authority (e.g., the Union Home Secretary), and such approval is subject to mandatory periodic reviews.

Taking into account the practices of the Indian public authorities, and the fact that BlackLine has never been subject to an Indian government request for access to customer Personal Data, BlackLine concludes that: (a) India surveillance laws and regulations that are potentially applicable to BlackLine's Processing of Personal Data are unlikely to be applied in practice to customer Personal Data Processed by BlackLine; and (b) consequently, BlackLine has no reason to believe that such laws and regulations will prevent BlackLine from fulfilling its obligations under the 2021 SCCs.

Conclusion

Based on the above, BlackLine has no reason to believe that the U.S., Australian, Singapore, Mexico or Indian laws and practices applicable to the Processing of Personal Data by BlackLine or its Sub-processors prevent BlackLine from fulfilling its obligations under the 2021 SCCs, the UK IDTA, Swiss Addendum to the 2021 SCCs or otherwise pose any materially different privacy risks as to inappropriate disclosure of personal data to foreign government law enforcement and intelligence agencies. Furthermore, we assess the severity of the risk of such a request breaching a Data Subject's rights as being very low.

In summary, we believe a combination of objective factors such as the business sectors in which BlackLine's Hosted Service is used, the purposes for which BlackLine transfers and Processes Personal Data, the limited amount of Personal Data Processed within BlackLine's Hosted Service and it's probable little interest to government intelligence agencies, the measures set forth in Step 4, relevant public statements issued by the relevant governments, publicly reported cases evidencing the past application of security laws, the documented experiences of other cloud service providers processing comparable personal data, evidence of practices by applicable government authorities, that surveillance laws and regulations that are potentially applicable to BlackLine's Processing of customer Personal Data are unlikely to be applied in practice, BlackLine's own experiences to date, and the improved protections introduced in the October 2022 Executive Order, all strongly support BlackLine's assessment that it can continue to provide adequate protection to data transferred from Europe to the U.S., Australia, Singapore, Mexico and India.

Even if BlackLine is compelled to respond to a law enforcement request for Personal Data, we will carefully review the request to verify it is lawful and challenge the request, if we conclude it is invalid or unlawful, in accordance with BlackLine's principles and contractual commitments on government access requests as outlined in Step 4 below.

This extensive review has been undertaken in line with the EDPB recommendations, which specifically lists these as reliable sources on the application of the law in practice. Therefore, no additional supplementary measures are necessary at this time.

4. Adopt "supplementary" technical, contractual and organizational measures to protect the personal data

This Step identified in the EDPB Recommendations is strictly only relevant if the assessment in Step 3 indicates that more is needed (i.e., in addition to the GDPR article 46 transfer mechanism relied on). As can be seen, BlackLine's assessment is that Personal Data is protected to the relevant standard. In addition, "supplementary" measures are not required where the recipient country benefits from a valid adequacy decision.

BlackLine has invested in privacy and security technical and organizational measures. Below, we have set out the technical, contractual, and organizational measures we have implemented to protect Personal Data, support the effectiveness of the 2021 SCCs and allow for a lawful transfer of Personal Data outside Europe using the Hosted Service.

A. Contractual Measures

BlackLine has incorporated the 2021 SCCs (including UK IDTA and Swiss Addendum) into its Data Processing Addendum and makes strong contractual commitments about the measures it takes and makes available to protect Personal Data. For example, BlackLine commits to:

- Technical and Organizational Measures. Implementing and maintaining technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, or alteration, and unauthorized access or disclosure;

- Data Subject Requests. Assisting customers in complying with their controller obligations under the GDPR in responding to Data Subject requests, and Customers can use their own access to the relevant Personal Data to comply with Data Subject requests;

- Audit Reports. Providing third-party certifications and audit reports so customers can verify BlackLine's compliance; and

- Government Access Requests. Extensive protections around compelled disclosure in respect of Personal Data.

B. Organizational Measures

● Policies and Procedures for Government Access Requests. As a general principle, BlackLine will not disclose Personal Data in response to government access requests unless it is either under a compelling legal obligation to do so or there is an imminent risk of serious harm that merits compliance. If a request concerns Personal Data for which a Customer is the Controller, we would ordinarily ask the requesting authority to direct their request to the relevant Customer and support the Customer in accordance with the terms of the DPA. These protections are offered to all Customers via our DPA, including Customers that have chosen to have their data hosted in Europe.

● Data minimization. As part of its Privacy by Design principles, BlackLine incorporates data minimization principles of adequacy, relevance, and limitation into the design of the development and operation of the Hosted Service. Operationally, BlackLine applies role-based least privilege access control restrictions for access to all Personal Data, such that BlackLine user access is restricted to the resources required for users as necessary to perform their duties. BlackLine makes use of verification mechanisms such as privacy and data security certifications and audit standards, including but not limited to ISO/IEC 27001. These demonstrate data minimization and organizational security measures that limit the data available for access and protect against unauthorized access.

C. Technical Measures

● Protect Against Unauthorized Disclosure. BlackLine has implemented technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, or alteration, and unauthorized access or disclosure.

● Best Practices. BlackLine follows information-security best practices and is certified under various standards, such as ISO/IEC 27001 (Information Security Management), ISO/IEC 27701 (Privacy Information Management), ISO/IEC 27017 (Cloud Security), ISO/IEC 27018 (Cloud Privacy), SSAE 18/ISAE 3402 SOC 1, SOC 2 and SOC 3. BlackLine's technical and organizational measures for customer Personal Data are set forth below. More information about BlackLine's technical and organizational measures is available here.

● ISMS. BlackLine maintains a comprehensive program of controls in the form of an Information Security Management System (ISMS). It includes policies,

procedures, and operational requirements for the implementation of a layered system of preventative, detective, and corrective controls. While the ISMS aims to ensure the confidentiality, integrity and availability of Personal Data Processed by BlackLine's Hosted Service, the most important goal of the ISMS is the protection of Personal Data and the ability to provide the Customer assurance regarding data protection.

● Encryption. BlackLine uses Transport Layer Security 1.2 (at a minimum) to encrypt Personal Data in transit over public networks between customers and BlackLine, and between BlackLine data centers. In addition to this, all Personal Data is encrypted at rest.

● Regional Data Storage. BlackLine offers Customers a way to store their data on a regional basis. BlackLine allows its Customers to select the data center region to store their Personal Data, including in Europe. BlackLine's Hosted Service is hosted on data centers maintained by industry-leading service providers, which offer state-of-the-art technical and organizational security measures designed to protect the data they host. The Hosted Service can be delivered through either public cloud (Google Cloud Platform/GCP) or regional private cloud data centers; data storage of Personal Data in both environments is encrypted both at rest and in transit. BlackLine uses AES256 to encrypt all Personal Data at rest. Customer files and databases are encrypted using best-of-breed commercial encryption tools in the data center environments, in addition to the native cloud hosting provider encryption technologies and key management services in the public cloud environments. Both sets of tools control access to encrypted information using a series of rules that ensure that only authorized applications and individuals can access Personal Data.

D. Encryption. A key technical measure described in the EDPB Recommendations is encryption, including the management of encryption keys. BlackLine offers enhanced encryption services that Customers can leverage to protect their Personal Data. BlackLine employs data security controls, including encryption for data at rest and in transit. If data is encrypted, it will be unreadable to a third party without the encryption key, and cannot be accessed in a meaningful form by a U.S. or other government agency unless they go through formal access channels. Encryption is therefore an effective means of preventing third-party access to BlackLine Personal Data except through a formal legal request to BlackLine and, depending on the type of encryption used, may even prevent access via formal legal channels. Encryption key management is carried out with using industry best practices.

● Encryption at rest. Personal Data at rest is encrypted by default using AES256 or a stronger alternative. BlackLine implements industry accepted

encryption algorithms that have keys that are no less than 256 bits for symmetric-key algorithms, 2048 bits for RSA based asymmetric-key algorithms, and 128 bits for elliptic curve based asymmetric-key algorithms.

● Encryption in transit. Personal Data transmitted via TLS can be encrypted with TLS 1.2 or stronger alternative supported. BlackLine APIs only accept connections over encrypted channels (e.g., TLS) and only for requests that are cryptographically identified (e.g., HMAC). BlackLine APIs are used for receipt of Personal Data from Customers. All data fields identified as secure in the API Documentation are transmitted and stored in accordance with these standards, rendering the data impractical to recover. SFTP, which gives Customers the choice of encryption algorithms (including AES256), can also be used to securely upload Personal Data.

E. No back doors or mass and indiscriminate access. BlackLine has never disclosed Personal Data in response to government requests. It would not do so without valid and compulsory legal process. Nor does BlackLine authorize government authorities from any jurisdiction to access Personal Data held in BlackLine's Hosted Service through mechanisms such as "back doors." BlackLine will oppose any attempt to require BlackLine to provide such access in accordance with BlackLine's DPA. BlackLine insists that all requests seeking Personal Data be presented to BlackLine and processed in accordance with applicable law and BlackLine policies. BlackLine's technical and organizational measures are designed to prevent mass or indiscriminate access to Personal Data while in transit.

F. Transparency. To date, BlackLine has never received any requests for access to Personal Data under Section 702 FISA. We are also not aware of any direct access to Personal Data under EO 12333.

5. Procedural steps necessary to implement effective supplementary measures

This Step is only relevant if the assessment in Step 3 indicated that more was needed and supplementary measures ought to have been taken. The measures nonetheless taken are in any case effective without any procedural step being needed. As far as the contractual measures described are concerned BlackLine offers the 2021 SCCs and the updated Data Processing Addendum to its new customers and is offering an easy solution to existing customers who want to upgrade to the new 2021 SCCs in advance of the European Commission's transition period of December 27, 2022. The updated Data Processing Addendum also includes the UK IDTA and Swiss Addendum to validate the 2021 SCCs for UK and Swiss data protection laws.

6. Re-evaluate at appropriate intervals

BlackLine regularly re-evaluates the level of protection afforded to Personal Data transferred to non-European countries' and, where necessary, adapt the measures it has implemented to address changing data protection regulatory and risk environments. We encourage our Customers to regularly re-evaluate the level of protection afforded to Personal Data transferred to non-European countries.

7. BlackLine Determines Equivalent Protection of Personal Data

As outlined above, when assessing potential data protection risks in relation to compelled disclosure and international data transfers post Schrems II, the GDPR requires that data importers and data exporters should take into account the specific circumstances of the transfer and any safeguards put in place (including relevant contractual, technical and organizational measures applying to the Personal Data). In other words, a holistic approach is required, in which the entire array of operational, contractual, technical and organizational security measures offered by BlackLine and those that can be implemented by Customers need to be considered, so that an appropriate risk assessment can be made. The GDPR does not require that organizations eliminate all risk, which would be impossible, but to take appropriate measures to mitigate risks. We believe to have such measures in place.

Questions

Any questions about this document or our data protection practices can be sent to the BlackLine Privacy Team at dpa.client@blackline.com.

We trust that this document sufficiently informs our customers and prospective customer on the related topic.

BlackLine Privacy

BlackLine Technical and Organizational Measures

Overview of the technical and organisational measures to be taken by BlackLine regarding the protection of Personal Data.

Physical Access Control

Measures to ensure that only those explicitly authorized will have physical access to systems used to process Personal Data.

- security guards, doormen
- keys and corresponding documentation
- electronic access control system
- video surveillance
- security checks for any external companies/services
- security checks for visitors
- security guidelines for utilization of mobile devices

System Access Control

***Measures to prevent data processing systems from being used without authorization*:**

- password guidelines (e.g., digits/special characters, min. length, expiration, uniqueness)
- multi-factor authentication
- automatic log-out or password-protected screensaver after certain period without user activity
- access authentication rules
- firewall, anti-virus protection
- intrusion detection/intrusion prevention
- logging of access
- securing external interfaces

Data Access Control

Measures to ensure that those authorized to use data processing systems have access only to those data they are authorized to access, and that Personal Data cannot be read, copied, altered or removed without authorization during processing, use and after:

- access control (access rights limited by profiles and roles)
- documentation of access rights
- approval and assignment of access rights through authorized personnel only

Data Transfer Control

Measures to ensure that Personal Data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred Personal Data using data transmission facilities:

- transport encryption
- encryption of physical data carriers

Data Entry Control

Measures to ensure that it is possible to check and ascertain whether Personal Data have been entered into, altered or removed from data processing systems and if so, by whom:

- documenting/logging of physical access
- logging of system access (*e.g.*, login name, IP address)
- logging of individual actions
- other event logging (*e.g.*, intrusion and hacking attempts, unsuccessful login attempts)

Availability Control

Measures to ensure that Personal Data are protected against accidental destruction or loss:

- backup in separate location and regular tests of recovery procedures
- business continuity/disaster recovery
- uninterruptable power supply (UPS)
- anti-theft measures
- fire protection (early-warning-fire-detection, extinguishing system)
- water protection
- redundant air conditioning system

Separation of Data

Measures to ensure that data collected for different purposes can be processed separately:

- clear physical and/or logical separation of data from data of other Controllers
- physical and/or logically separated systems for development and production environments
- pseudonymisation of data, where appropriate